FIG. 1

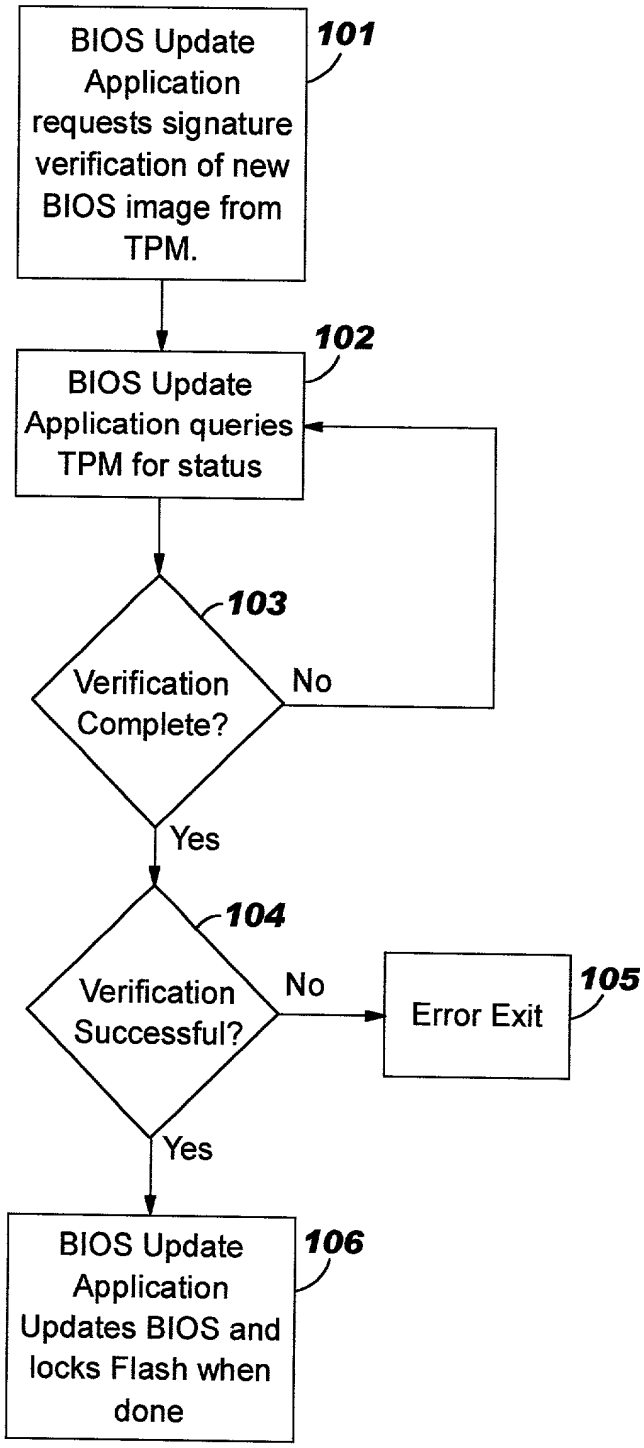

FIG. 2

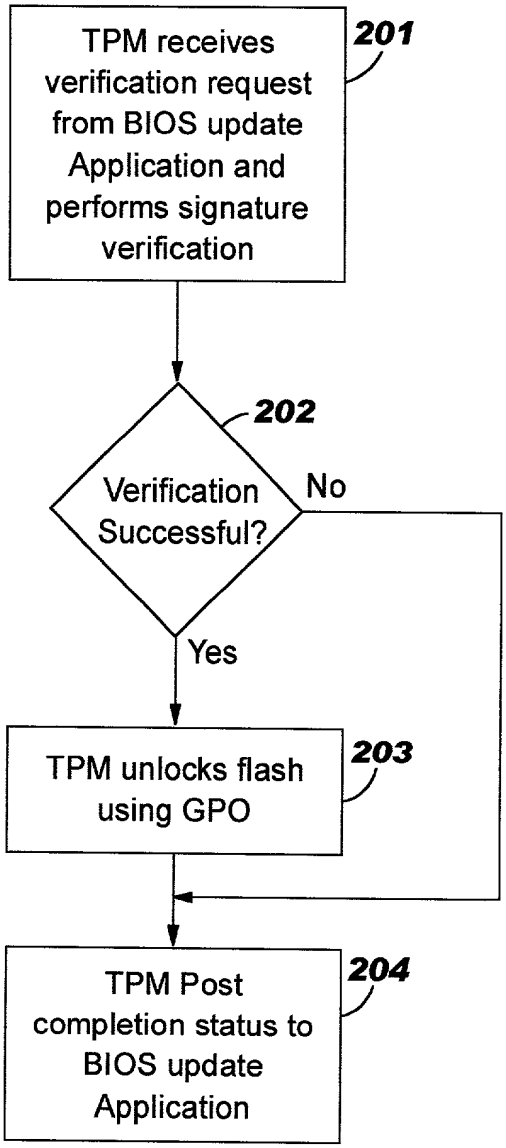
TPM receives verification request from BIOS update Application and performs signature verification
201
202
Verification Successful?
No
Yes
TPM unlocks flash using GPO
203
TPM Post completion status to BIOS update Application
204

FIG. 3